UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

RICHARD WEBSTER, individually and on behalf of all others similarly situated, Plaintiff, v. **ADVOCATE AURORA HEALTH, INC.** Defendant.	Case No. Judge **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiff Richard Webster ("Plaintiff"), individually and on behalf of all others similarly situated ("Class Members") brings this Class Action Complaint against Advocate Aurora Health, Inc. ("Advocate" or "Defendant"), and alleges, upon personal knowledge as to his own actions, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Defendant is one of the largest healthcare systems in country. As a condition of receiving healthcare, Defendant's patients (i.e., Plaintiff and Class Members) entrust it with scores of personally identifiable information ("PII") and protected health information ("PHI") (collectively, "Private Information"). Unbeknownst to Plaintiff and Class Members, Defendant intentionally configured and implemented a software device known as a Tracking Pixel (the "Pixel") to collect and transmit information from its website to third parties without consent, including information communicated in sensitive and presumptively confidential patient portals and mobile apps like its MyChart portal and LiveWell app.[1]

2. As a result of the Pixel deployed by Defendant, Plaintiff's and Class Members

[1] *See* https://www.jsonline.com/story/news/2022/10/21/advocate-aurora-health-data-breach-could-impact-3-million-patients/69581723007/

Private Information was compromised and disclosed to third parties, including their full names, email addresses, phone numbers, computer IP addresses, emergency contact information, appointment information, medical provider information, medical histories, and other information submitted on Defendant's website and patient portal (the "Data Breach").[2]

3. A pixel is a piece of code used to collect marketing data, such as measuring the activity on a webpage. A pixel operates by embedding code in each page a visitor to the website views. The code captures vast amounts of information, such as webpage name and how visitors interact with the page, including which buttons they click and the information they enter into form fields (which can include contact and medical information). Pixels also capture search queries, visitor IP addresses, and browser identifiers.[3]

4. The Pixel employed by Defendant here is a software device created by Meta Platforms, Inc., formerly known as Facebook, Inc., a company with its own dubious reputation for data security and privacy. The Defendant's use of the Pixel caused Plaintiff's and Class Members' Private Information to be shared with Facebook and other marketing partners.

5. In the course of their relationship with Defendant, Plaintiff and Class Members never consented, agreed, authorized, or otherwise permitted Defendant to disclose their Private Information or to assist with intercepting communications they reasonably believed to be confidential and only between themselves and their healthcare providers. At no point were Plaintiff and Class Members provided with any written notice that Defendant discloses its website users' Private Information, nor were they provided any means of opting out of such disclosures. Despite this, Defendant knowingly disclosed Plaintiff's and Class Members' Private Information to Facebook.

---

[2] *See* https://www.advocateaurorahealth.org/; https://www.livewellaah.org/?#open-frame
[3] https://developers.facebook.com/docs/meta-pixel/

6. Defendant did not disclose that it had transmitted patients' sensitive and non-public Private information to unauthorized third parties until on or about October 20, 2022, when it sent Notice of Data Breach letters ("Notice") and posted a notice on its website.

7. Healthcare providers like Defendant that collect and store Private Information have statutory, regulatory, contractual, and common law duties to safeguard that information and to ensure it remains private. Healthcare providers also have a fiduciary duty to keep the Private Information of their patients confidential and protected from disclosure. Defendant's knowing implementation of tracking software that collects and discloses Private Information to third parties and marketers is an egregious breach of that duty.

8. Defendant knowingly implemented and configured the Pixel to disclose the identities and communications of its patients to Facebook. Facebook's get started page clearly discloses that the Pixel "relies on Facebook cookies, which enable us to match your website visitors to their respective Facebook User accounts. Once matched, we can tally their actions in the Facebook Ads Manager so you can use the data to analyze your website's conversion flows and optimize your ad campaigns."[4] Accordingly, Defendant chose to incorporate code on its website knowing that the code was intended to specifically identify its patients to Facebook alongside their Private Information and geographic location.

9. Defendant disregarded Plaintiff's and Class Members' rights by intentionally, willfully, recklessly, and/or negligently disclosing its patients' Private Information via the tracking Pixel. As a result, Plaintiff's and Class Members' Private Information was compromised through disclosure to Meta, Facebook, Google, and other unknown and unauthorized third parties. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains

[4] https://developers.facebook.com/docs/meta-pixel/get-started

confidential and disclosed only according to a patient's authorization, thus entitling them to injunctive and other equitable relief. Plaintiff and Class Members are also entitled to damages in an amount to be proven at trial.

10. Plaintiff asserts claims on behalf of himself and the Class Members for (1) invasion of privacy, (2) breach of contract, (3) breach of fiduciary duty, and (4) violations of Wis. Stat. § 146.81 *et seq.*

PARTIES

11. Plaintiff Richard Webster is a citizen and resident of West Bend, Wisconsin.

12. Defendant Advocate Aurora Health is a not-for-profit corporation incorporated in Delaware with its principal place of business at 750 W. Virginia St. P.O. Box 341880, Milwaukee, Wisconsin 53204.

JURISDICTION AND VENUE

13. This Court has subject matter and diversity jurisdiction over this action under 28U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant to establish minimal diversity.

14. The Eastern District of Wisconsin has personal jurisdiction over the Defendant named in this action because one of Defendant's headquarters is in this District and Defendant conducts substantial business in this District through its headquarters, offices, parents and/or affiliates.

15. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant and/or its parents or affiliates are headquartered in this District and a substantial part of the events

or omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

Background

16. According to Defendant, it has 27 hospitals and more than 500 sites of care, with 75,000 employees, including 10,000 employed physicians in 2021, making it one of the largest healthcare providers in the country.[5]

17. Defendant serves patients via digital platforms, such as MyChart and LiveWell. These digital tools allow patients to schedule appointments or procedures, communicate with their healthcare providers, review their medical histories, and perform other healthcare focused communications.

18. Plaintiff and Class Members relied on the sophistication of Defendant's healthcare business to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

19. Nevertheless, the Pixel and other tracking software that Defendant installed on its healthcare portals tracks users as they navigate through the website and applications and logs which pages are visited, which buttons are clicked, specific information users enter into forms (e.g., name, home address, phone number, email address), search queries (e.g., "do I have covid"), and other information including a patient's IP address.[6] As more fully explained below, this information is collected not just by Defendant but also by Facebook because the Pixel Defendant embeds into its website, simultaneously transmits all the information it receives to Facebook.[7] If

[5] https://www.advocateaurorahealth.org/our-story/
[6] https://developers.facebook.com/docs/meta-pixel/
[7] Defendant acknowledges that the tracking software it implemented on its website likely disclosed the Private Information to Google and other companies.

the patient is also a Facebook user, Facebook in turn links the information they receive to the patient's Facebook profile, which includes other identifying information.

20. Defendant encourages its patients to use these digital tools and promotes the convenience and comprehensive functionality of the platforms. Defendant promises that "[y]ou can use the LiveWell with Advocate Aurora Health app or website (formerly the MyAdvocateAurora website) to manage your health and access the care you need, when you need it. You'll be able to schedule appointments, message your doctor, view test results, pay your bills or renew prescriptions online."[8]

Defendant Promised to Safeguard Private Information

21. Defendant promised its patients that "the LiveWell with Advocate Aurora Health app and website are secure environments. For more information, see our privacy policy."[9]

22. Defendant's Privacy Policy applies to any personal information provided to Defendant and any personal information that Defendant collects from other sources.

23. Defendant's Privacy Policy does not permit Defendant to use and disclose Plaintiff's and Class Members' Private Information for marketing purposes without written permission.

24. The Advocate Aurora Health Notice of Privacy Practices states, "This notice applies to any health care facility, medical staff, medical group or other health care entity now or in the future controlled by or under common control with Advocate Aurora Health and any of its affiliates or subsidiaries (collectively referred to as "Advocate Aurora Health" and designated as an Affiliated Covered Entity)."[10]

---

[8] advocateaurorahealth.org/livewell/faq#for-advocate-patients

[9] http://web.archive.org/web/20211220195147/https://www.advocateaurorahealth.org/livewell/faq#security-sign-in (as reflected on December 21, 2021)

[10] https://www.advocateaurorahealth.org/notice-of-privacy-practices/

25. The Advocate Health Care Privacy Policy states, "Advocate Health Care does not sell, trade or rent personal information about its website visitors."[11]

26. The Advocate Health Care Privacy Policy further represents as follows:

> "Examples of how you might provide us with such personal information include: Completing a survey or feedback form; Email us with a comment or question; Subscribing to our email notification service for new editions of Health Advocate magazine; Establishing a personalized homepage via our website; Making an online appointment / requestion an appointment; Engaging in an online dialogue via chat; Completing an online bill payment; Scheduling and/or use of Virtual Visits; Preforming online check-in; Using site-based wayfinding functions.
> …
>
> Our web server automatically collects and records the following information: Aggregate information on what pages are accessed; Address of the website that linked to us (referral URL); Date and time you access our site; Name and release number of web browser software used; Operating system used; Visitor's domain name, but not the email address; Visitor's IP address; Age, gender and interests.
> …
>
> This site recognizes and collects, when possible, the domain name of a visitor's server (for example, advocatehealth.com or aol.com). We do not automatically collect the full email address of visitors to our website. The only way we obtain your name or email address is when you choose to provide that information to us. Examples of how you might provide us with such personal information include: Completing a survey or feedback form; Email us with a comment or question; Subscribing to our email notification service for new editions of Health Advocate magazine; Establishing a personalized homepage via our website.
> …
>
> How do we use the information we collect? Advocate Health Care does not sell, trade or rent personal information about its website visitors.
> …
>
> Information provided to schedule online appointment, pay online bills, chat, virtual visits and other web functions may be transferred to 3rd party vendors and partners to continue service.
> ...
>
> Data collection: You may browse many areas of our website, including our home page, without disclosing any personal information about yourself. Within these areas we only collect and store the information that is automatically recognized by the Web server, such as your IP address and files you request from the server.

[11] https://www.advocatehealth.com/privacy-policy/

…

> We collect the personal data that you volunteer on registration(s), survey, online chat, online bill pay, virtual/telehealth visits, or other forms, or by email. Additionally, some areas of our website might be available only to certain persons and will require a login and password to access these areas. In order to be granted a login and password you may be asked some demographic information about yourself.
> …
>
> Data analysis: As described above, we sometimes collect anonymous information from visits to our site to help us provide better customer service. For example, we measure visitor activity on our website, but we do so in ways that keep the information anonymous. We use the information that we collect to measure the number of visitors to the different areas of our site and to help us make our site more useful to visitors. This includes analyzing these logs periodically to measure the traffic through our servers, the number of pages visited and the level of demand for pages and topics of interest. The logs may be preserved indefinitely and used at any time and in any way to prevent security breaches and to ensure the integrity of the data on our servers.
> …
>
> Cookies & other technologies: We collect the anonymous information we mentioned above through the use of various technologies, one of which is called "cookies". A cookie is an element of data that the website can send to your browser, which may then be stored on your hard drive. Cookies may last for only a single session or may span multiple sessions. We use cookies to track user activity by our registered users. Finally, cookies are employed in other applications that require the storage of user data from one screen to the next."[12]

27. Defendant violated its own Privacy Policy by unlawfully disclosing Plaintiff's and Class Members' Private Information to Facebook, Meta, and likely other third parties. Defendant further misrepresented that it would preserve the confidentiality of their Private Information and the anonymity of their identities.

The Data Breach

28. On or about October 20, 2022, Defendant posted a "Breach Notification" on its website.

[12] *Id.*

29. The Notice of Data Breach informed Plaintiff and Class Members (in substantially the same form) of the breach:

> Advocate Aurora Health is writing to provide transparency in its previous use of the Internet tracking technologies, such as Google and Meta (Facebook), that we and many others in our industry had implemented to understand how patients and others interact with our websites. These technologies disclose certain details about interactions with our websites, particularly for users that are concurrently logged into their Google or Facebook accounts and have shared their identity and other surfing habits with these companies. When using some Advocate Aurora Health sites, certain protected health information ("PHI") would be disclosed in particular circumstances to specific vendors because of pixels on our websites or applications. Information about these technologies and steps that individuals may take to further protect their health information can be found in our FAQ.
>
> In an effort to deliver high quality services to its community, Advocate Aurora Health uses the services of several third-party vendors to measure and evaluate information concerning the trends and preferences of its patients as they use our websites. To do so, pieces of code known as "pixels" were included on certain of our websites or applications. These pixels or similar technologies were designed to gather information that we review in aggregate so that we can better understand patient needs and preferences to provide needed care to our patient population. We learned that pixels or similar technologies installed on our patient portals available through MyChart and LiveWell websites and applications, as well as on some of our scheduling widgets, transmitted certain patient information to the third-party vendors that provided us with the pixel technology. We have disabled and/or removed the pixels from our platforms and launched an internal investigation to better understand what patient information was transmitted to our vendors.
>
> Out of an abundance of caution, Advocate Aurora Health has decided to assume that all patients with an Advocate Aurora Health MyChart account (including users of the LiveWell application), as well as any patients who used scheduling widgets on Advocate Aurora Health's platforms, may have been affected. Users may have been impacted differently based on their choice of browser; the configuration of their browsers; their blocking, clearing or use of cookies; whether they have Facebook or Google accounts; whether they were logged into Facebook or Google; and the specific actions taken on the platform by the user.
>
> The following information may have been involved: your IP address; dates, times, and/or locations of scheduled appointments; your proximity to an Advocate Aurora Health location; information about your provider; type of appointment or procedure; communications between you and others through MyChart, which may have included your first and last name and your medical record number; information about whether you had insurance; and, if you had a proxy MyChart account, your first name and the first name of your proxy. Based on our

> investigation, no social security number, financial account, credit card, or debit card information was involved in this incident.
>
> We have disabled and/or removed tracking pixels on patient websites and applications, and we are continuing to evaluate how to further mitigate the risk of unauthorized disclosures of patient protected health information in the future. We will continue to monitor our information security systems and make improvements and enhancements where appropriate. To the extent any tracking technologies are proposed in the future, such technologies will be evaluated under Advocate Aurora's enhanced, robust technology vetting process consistent with our commitments to patient privacy.[13]

30. Defendant advised that the information potentially impacted in the Data Breach included:

> your IP address; dates, times, and/or locations of scheduled appointments; your proximity to an Advocate Aurora Health location; information about your provider; type of appointment or procedure; communications between you and others through MyChart, which may have included your first and last name and your medical record number; information about whether you had insurance; and, if you had a proxy MyChart account, your first name and the first name of your proxy. Based on our investigation, no social security number, financial account, credit card, or debit card information was involved in this incident.[14]

31. There is a potential that more information was disclosed to Meta, Facebook, Google, and others during the two years data was submitted to Meta from Defendant's system.

32. Facebook describes itself as a "real identity platform,"[15] meaning users are allowed only one account and must share "the name they go by in everyday life."[16] To that end, when creating an account, users must provide their first and last name, along with their birthday and gender.[17]

---

[13] https://www.advocateaurorahealth.org/pixel-notification/
[14] *Id.*
[15] Sam Schechner and Jeff Horwitz, How Many Users Does Facebook Have? The Company Struggles to Figure It Out, WALL. ST. J. (last accessed October 2022).
[16] https://www.facebook.com/communitystandards/integrity_authenticity
[17] https://www.facebook.com/

33. Facebook sells advertising space by highlighting its ability to target users.[18] Facebook can target users so effectively because it surveils user activity both on and off its site.[19] This allows Facebook to make inferences about users beyond what they explicitly disclose, like their "interests," "behavior," and "connections."[20] Facebook compiles this information into a generalized dataset called "Core Audiences," which advertisers use to apply highly specific filters and parameters for their targeted advertisements.[21]

34. In 2021, Facebook generated $117 billion in revenue.[22] Roughly 97% of that came from selling advertising space.[23]

35. Advertisers can also build "Custom Audiences."[24] Custom Audiences enables advertisers to reach "people who have already shown interest in [their] business, whether they're loyal customers or people who have used [their] app or visited [their] website."[25] With Custom Audiences, advertisers can target existing customers directly, and they can also build a "Lookalike Audiences," which "leverages information such as demographics, interests, and behavior from your source audience to find new people who share similar qualities."[26] Unlike Core Audiences, advertisers can build Custom Audiences and Lookalike Audiences only if they first supply Facebook with the underlying data. They can do so through two mechanisms: by manually uploading contact information for customers, or by utilizing Facebook's "Business Tools."[27]

---

[18] https://www.facebook.com/business/help/205029060038706
[19] https://www.facebook.com/business/help/742478679120153?id=1205376682832142
[20] https://www.facebook.com/business/ads/ad-targeting
[21] https://www.facebook.com/business/news/Core-Audiences
[22]https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx
[23] *Id.*
[24] https://www.facebook.com/business/help/744354708981227?id=2469097953376494
[25] https://www.facebook.com/business/ads/ad-targeting
[26]https://www.facebook.com/business/help/164749007013531?id=401668390442328
[27]https://www.facebook.com/business/help/170456843145568?id=2469097953376494; https://www.facebook.com/business/help/1474662202748341?id=2469097953376494.

36. As Facebook puts it, the Business Tools "help website owners and publishers, app developers and business partners, including advertisers and others, integrate with Facebook, understand and measure their products and services, and better reach and serve people who might be interested in their products and services."[28] Put more succinctly, Facebook's Business Tools are bits of code that advertisers can integrate into their website, mobile applications, and servers, thereby enabling Facebook to intercept and collect user activity on those platforms.

37. The Business Tools are configured to capture certain data, like when a user visits a webpage, that webpage's Universal Resource Locator ("URL") and metadata, or when a user downloads a mobile application or makes a purchase.[29] Facebook's Business Tools can also track other events. Facebook offers a menu of "standard events" from which advertisers can choose, including what content a visitor views or purchases.[30] Advertisers can even create their own tracking parameters by building a "custom event."[31]

38. One such Business Tool is the Facebook Tracking Pixel which Defendant implemented on its digital platforms. Facebook offers this piece of code to advertisers, like Defendant, to integrate into its website. As the name implies, the Facebook Pixel "tracks the people and type of actions they take."[32] When a user accesses a website hosting the Facebook Pixel, Facebook's software script surreptitiously directs the user's browser to send a separate message to Facebook's servers. This second, secret transmission contains the original request sent to the host website, along with additional data that the Facebook Pixel is configured to collect. This

[28] https://www.facebook.com/help/331509497253087.
[29] *See* https://developers.facebook.com/docs/facebook-pixel/advanced/; *see also* https://www.facebook.com/business/help/218844828315224?id=1205376682832142; https://developers.facebook.com/docs/marketing-api/app-event-api/
[30] https://www.facebook.com/business/help/402791146561655?id=1205376682832142
[31] https://www.facebook.com/business/help/964258670337005?id=1205376682832142; *see also* https://developers.facebook.com/docs/marketing-api/app-event-api/
[32] https://www.facebook.com/business/goals/retargeting

transmission is initiated by Facebook code and concurrent with the communications with the host website. Two sets of code are thus automatically run as part of the browser's attempt to load and read Defendant's websites – Defendant's own code, and Facebook's embedded code.

39. An example illustrates the point. Take an individual who navigates to Defendant's website and clicks on the "Check Symptoms & Find COVID-19 Care" tab. When that tab is clicked, the individual's browser sends a request to Defendant's server requesting that server to load the particular webpage. Because Defendant utilizes the Facebook Pixel, Facebook's embedded code, written in JavaScript, sends secret instructions back to the individual's browser, without alerting the individual that this is happening. Facebook causes the browser to secretly duplicate the communication with Defendant, transmitting it to Facebook's servers, alongside additional information that transcribes the communication's content and the individual's identity.

40. For example, if the user clicks "Find a Doctor" and enters their Zip Code and the doctor's specialty, like "Addiction Medicine," this is information is shared with Facebook, Google, or others that Defendant has configured its Pixel to interact with.

41. After collecting and intercepting this information, Facebook processes it, analyzes it, and assimilates it into datasets like Core Audiences and Custom Audiences.

42. Every time Defendant sends a patient's website activity data to Facebook, that patient's personally identifiable information is also disclosed, including their Facebook ID ("FID"). An FID is a unique and persistent identifier that Facebook assigns to each user. With it, anyone can look up the user's Facebook profile and name. Notably, while Facebook can easily identify any individual on its Facebook platform with only their unique FID, so too can any ordinary person who comes into possession of an FID. Facebook admits as much on its website. Indeed, ordinary persons who come into possession of the FID can connect to the corresponding

Facebook profile and the persons real world identity. A user who accesses Defendant's digital platforms while logged into Facebook will transmit the user cookie to Facebook, which contains that user's unencrypted Facebook ID.

43. Google and other companies likewise process this data in a similar manner and use it to connect the information to particular individuals to build marketing and other data profiles.

44. Through the Pixel, Defendant Advocate shares its patients' identities and online activity, including personal information and search results related to their private medical treatment.

45. Defendant could have configured its tracking software to limit the information that it communicated to third parties but it did not and instead intentionally selected the features and functionality of the Pixel that resulted in the Data Breach.

46. Plaintiff never consented, agreed, authorized, or otherwise permitted Defendant Advocate to disclose his Private Information and assist with intercepting his communications. Plaintiff was never provided with any written notice that Defendant discloses its patients' protected health information, nor was he provided any means of opting out of such disclosures. Defendant nonetheless knowingly disclosed Plaintiff's protected health information to Meta, Facebook, Google, and other unauthorized entities.

47. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for legitimate healthcare purposes only, and to make only authorized disclosures of this information.

48. By law, Plaintiff is entitled to privacy of his protected health information and confidential communications. Defendant deprived Plaintiff and Class Members of their privacy

rights when it: (1) implemented a system that surreptitiously tracked, recorded, and disclosed Plaintiff's and Class Members' confidential communications, personally identifiable information, and protected health information; (2) disclosed patients' protected information to Facebook and others—unauthorized third-party eavesdroppers; and (3) undertook this pattern of conduct without notifying Plaintiff and Class Members and without obtaining their express written consent. Plaintiff did not discover that Defendant disclosed their personally identifiable information and protected health information to Facebook, and assisted Facebook with intercepting their communications

Plaintiff's Richard Webster's Experience

49. Plaintiff Richard Webster received healthcare services from one of the hospitals in Defendant's network and that relied on Defendant's digital healthcare platforms to communicate confidential patient information.

50. Over the past two years, Plaintiff used Defendant's digital tools to receive healthcare services from Defendant and at Defendant's direction and encouragement. Plaintiff reasonably expected his online communications with Advocate were confidential, solely between himself and Advocate, and that such communications would not be transmitted to or intercepted by a third party.

51. Plaintiff provided his Private Information to Defendant and trusted that the information would be safeguarded according to Advocate's privacy policies and state and federal law.

52. As described herein, Defendant sent Plaintiff's Private Information to Facebook, Google, and others after Plaintiff used Defendant's digital platforms to communicate healthcare and identifying information to Defendant.

53. Through the process described herein, Defendant assisted Facebook, Google, and others with intercepting Plaintiff communications, including those that contained personally identifiable information, protected health information, and related confidential information. Advocate facilitated these interceptions without Plaintiff's knowledge, consent, or express written authorization.

CLASS ALLEGATIONS

54. Plaintiff brings this nationwide class action on behalf of themselves and on behalf of others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

55. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> **All persons Defendant identified as being among those impacted by the Data Breach, including all who were sent a notice of the Data Breach.**

56. Plaintiff also seeks to represent a subclass of Wisconsin residents (the "Wisconsin Subclass"), defined as follows:

> **All Wisconsin residents Defendant identified as being among those impacted by the Data Breach, including all who were sent a notice of the Data Breach.**

57. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

58. Plaintiff reserves the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

59. Numerosity, Fed R. Civ. P. 23(a)(1): Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are, at the very least, thousands of individuals in both the Nationwide Class and Wisconsin Subclass whose Private Information was improperly accessed in the Data Breach, and each Class is apparently identifiable within Defendant's records.

60. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Class exists and predominates over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect Plaintiff's and Class Members' Private Information;

b. Whether Defendant had duties not to disclose the Plaintiff's and Class Members' Private Information to unauthorized third parties;

c. Whether Defendant had duties not to use Plaintiff's and Class Members' Private Information for non-healthcare purposes;

d. Whether Defendant had duties not to use Plaintiff's and Class Members' Private Information for unauthorized purposes;

e. Whether Defendant failed to adequately safeguard Plaintiff's and Class Members' Private Information;

f. Whether and when Defendant actually learned of the Data Breach;

g. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

h. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their Private Information had been compromised;

i. Whether Defendant failed to properly implement and configure the tracking software on its digital platforms to prevent the disclosure of information compromised in the Data Breach;

j. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

k. Whether Defendant engaged in unfair, unlawful, or deceptive practices by misrepresenting that it would safeguard Plaintiff's and Class Members' Private Information;

61. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their Private Information compromised as a result of the Data Breach, due to Defendant's use and incorporation of the tracking software.

62. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

63. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seek no

relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff have suffered are typical of other Class Members. Plaintiff have also retained counsel experienced in complex class action litigation, and Plaintiff intend to prosecute this action vigorously.

64. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

65. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary

and duplicative of this litigation.

66. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

67. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

68. Unless a Class-wide injunction is issued, Defendant may continue in their failure to properly secure and unlawful disclosure of the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

69. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

70. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private

Information;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to the disclosure of patient information;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and Class Members' Private Information;

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

COUNT I
INVASION OF PRIVACY

71. Plaintiff repeats and re-alleges each and every allegation in the Complaint as if fully set forth herein.

72. Plaintiff brings this claim on behalf of himself and the Nationwide Class, or alternatively, the Wisconsin Subclass.

73. Plaintiff and Class Members had a reasonable expectation of privacy in their communications with Defendant via its website and the communications platforms and services therein.

74. Plaintiff and Class Members communicated Private Information that they intended for only Defendant to receive and that they understood Defendant would keep private.

75. Defendant's use of the Pixel and disclosure of the substance and nature of communications to third parties without the knowledge and consent of Plaintiff and Class members is an intentional intrusion on Plaintiff's and Class members' solitude or seclusion.

76. Plaintiff and Class members had a reasonable expectation of privacy given Defendant's representations, HIPAA Notice of Privacy Practices and Privacy Policy. Moreover, Plaintiff and Class members have a general expectation that their communications regarding healthcare with their healthcare providers will kept confidential. Defendant's disclosure of private medical information coupled with individually identifying information is highly offensive to the reasonable person.

77. As a result of Defendant's actions, Plaintiff and Class members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

78. Plaintiff and Class members have been damaged as a direct and proximate result of Defendant's invasion of their privacy and are entitled to just compensation, including monetary damages.

79. Plaintiff and Class members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiff and Class members for the harm to their privacy interests as a result of its intrusions upon Plaintiff's and Class members' privacy.

80. Plaintiff and Class members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendant's actions, directed at injuring Plaintiff and Class members in conscious disregard of their rights. Such damages are needed to deter Defendant's from engaging in such conduct in the future.

81. Plaintiff also seek such other relief as the Court may deem just and proper.

COUNT II
BREACH OF CONTRACT

82. Plaintiff repeats and re-alleges each and every allegation in the Complaint as if fully set forth herein.

83. Plaintiff brings this claim on behalf of himself and the Nationwide Class, or alternatively, the Wisconsin Subclass.

84. Defendant required Plaintiff and the Class Members to provide their Private Information, including names, email addresses, phone numbers, computer IP addresses, and emergency contact information, appointment information, and other content submitted into Defendant's website as a condition of their receiving healthcare services.

85. As a condition of utilizing Defendant's digital platforms and receiving services from Defendant, Plaintiff and the Class provided their Private Information and compensation for their medical care. In so doing, Plaintiff and the Class entered into contracts with Defendant by which Defendant agreed to safeguard and protect such information, in its Privacy Policies and elsewhere, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

86. Plaintiff and the Class Members fully performed their obligations under the contract with Defendant.

87. Upon information and belief, Defendant's relevant privacy policies and

representations require it to take appropriate steps to safeguard the Private Information entrusted to it by the Plaintiff and Class Members.

88. Defendant breached these agreements, which directly and/or proximately caused Plaintiff and Class Members to suffer damages, including nominal damages.

89. Defendant breached the contracts it made with Plaintiff and the Class by failing to safeguard and protect their Private Information, and by failing to provide timely and accurate notice to them that the Private Information was compromised as a result of the Data Breach.

As a direct and proximate result of Defendant's above-described breach of contract, Plaintiff and the Class have suffered (and will continue to suffer) the compromise and disclosure of their Private Information and identities.

90. As a direct and proximate result of Defendant's above-described breach of contract, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT III
BREACH OF FIDUCIARY DUTY

91. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

92. Plaintiff brings this claim on behalf of himself and the Nationwide Class, or alternatively, the Wisconsin Subclass.

93. A relationship existed between Plaintiff and the Class one the one hand and Defendant on the other in which Plaintiff and the Class put their trust in Advocate to protect the Private Information of Plaintiff and the Class and Advocate accepted that trust.

94. Defendant Advocate breached the fiduciary duty that it owed to Plaintiff and the Class Members by failing to act with the utmost good faith, fairness, and honesty, failing to act

with the highest and finest loyalty, and failing to protect, and intentionally disclosing, the Private Information of Plaintiff and the Class.

95. Defendant's breach of fiduciary duty was a legal cause of damage to Plaintiff and the Class.

96. But for Defendant's breach of fiduciary duty, the damage to Plaintiff and the Class would not have occurred.

97. Defendant's breach of fiduciary duty contributed substantially to producing the damage to the Plaintiff and the Class.

98. As a direct and proximate result of Defendant's breach of fiduciary duty, Plaintiff and Class Members are entitled to and do demand actual, consequential, and nominal damages, injunctive relief, and all other relief allowed by law.

COUNT IV
VIOLATION OF CONFIDENTIALITY OF PATIENT HEALTH CARE RECORDS
Wis. Stat. § 146.81 et seq.

99. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

100. Plaintiff brings this claim on behalf of himself and the Wisconsin Subclass (for purposes of this claim, referred to as the "Class").

101. Under Wisconsin law all patient health care records must remain confidential and patient health care records may only be released to a person upon the informed consent of the patient, or as authorized by the patient.

102. Defendant disclosed the private and protected medical information of Plaintiff and Class Members to unauthorized third parties without their knowledge, consent, or authorization.

103. Advocate is a healthcare provider as defined by Wis. Stat. Ann. § 146.816(1).

104. Plaintiff and Class Members are patients, and, as a health care provider, Advocate had and has an ongoing obligation not to disclose their Private Information.

105. The Private information disclosed by Defendant is protected health information as defined by Wis. Stat. Ann. § 146.816(f).

106. Defendant violated Wis. Stat. § 146.81, *et seq* through its willful and knowing failure to maintain and preserve the confidentiality of the medical information of Plaintiff and the Class. Defendant's conduct with respect to the disclosure of its patients confidential Private Information was willful and knowing because Defendant configured and implemented the digital platforms and tracking software that gave rise to the Data Breach.

107. Plaintiff and Class Members were injured as a result of Advocate's violation of the confidentiality of patient health care law.

108. As a result of its intentional and willful disclosure of Plaintiff and Class Members' Private Information, Defendant is liable for actual damages, additional damages of at least $25,000 if the violation was willful or $1,000 otherwise, and the costs and attorneys' fees incurred as a result of the violation. Wis. Sta. Ann. § 146.84.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a) For an Order certifying this action as a Class action and appointing Plaintiff as Class Representatives and Plaintiff's counsel as Class Counsel;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt,

complete and accurate disclosures to Plaintiff and Class Members;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Sensitive Information compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e) Ordering Defendant's to pay for not less than three years of credit monitoring services for Plaintiff and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law; For an award of punitive damages, as allowable by law;

g) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

h) Pre- and post-judgment interest on any amounts awarded; and

i) Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

/s/ *Joseph M. Lyon*
Joseph M. Lyon
THE LYON LAW FIRM, LLC
2754 Erie Ave.
Cincinnati, OH 45208
Phone: (513) 381-2333
Fax: (513) 766-9011
jlyon@thelyonfirm.com

Terence R. Coates (*pro hac vice* forthcoming)
Dylan J. Gould (*pro hac vice* forthcoming)
MARKOVITS, STOCK & DEMARCO, LLC
119 East Court Street, Suite 530
Cincinnati, OH 45202
Telephone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
dgould@msdlegal.com